

the unique human identifiers constitute secure endorsed transactions;

wherein the transmitting step includes the substep of formatting the unique codes, the transaction data, and the unique human identifiers to produce single whole representations of secure endorsed transactions.

Claim 9, line 1, change "8" to --5--;

Claim 14, line 5, change "memory" to --storage--.

REMARKS

In the Office Action, the Examiner objected to claims 3, 4, and 14, rejected claims 1-4 and 24-27 under 35 U.S.C. § 103(a) as being unpatentable over Donald W. Davies "Use of a 'Signature Token' to Create a Negotiable Document" ("Davies") in view of U.S. Patent No. 4,825,050 to Griffith et al. ("Griffith"); and rejected claims 5-23 and 29-31 under 35 U.S.C. § 103(a) as being unpatentable over Davies in view of Griffith and further in view of U.S. Patent No. 5,689,565 to Spies ("Spies").

By this amendment, Applicants propose to cancel claim 2, amend claims 3, 4, and 14 to correct for antecedent basis problems noted by the Examiner, and to amend claim 1 to include the limitations of canceled claim 2.

Regarding the rejection of claim 1 as being unpatentable over Davies in view of Griffith, Applicants respectfully traverse this rejection. Claim 1 has been amended to incorporate the limitations of dependent claim 2. The amendment to claim 1 does not raise new issues, as all of the limitations of amended claim 1 were expressly part of claim 2.

Claim 1, as amended, is directed to a combination of steps including generating a unique code from the transaction data *and* the unique human identifier and formatting the unique code, the transaction data, *and* the unique human identifier to produce a single whole representation of a secure endorsed transaction. Therefore, the source of the claimed unique code is *both* the transaction data *and* the unique human identifier. Further, the formatting step includes the unique code, the transaction data, and the unique human identifier. The prior art cited by the Examiner fails to teach or suggest using both transaction data and a unique human identifier to produce a unique code and then formatting the unique code with transaction data and a unique human identifier.

At page 3 of the Office Action, the Examiner cites Davies as teaching:

receiving transaction data (9, 10, 11, 12, 14, and 15) corresponding to a transaction and at least one unique identifier of a customer (typically a human) (5); and generating a unique code 16 from the transaction data and the unique identifier of a customer, wherein the unique code constitutes a secure endorsement of the transaction by the party corresponding to the unique identifier (5).

The Examiner, however, has misinterpreted the teachings of Davies. There is no teaching or suggestion of generating a unique code from transaction data and a unique identifier. The Examiner cites customer identity 5 of Davies as a unique identifier and signature 16 of Davies as the unique code.

Davies teaches at page 378, "a 'smart card' . . . capable of generating a digital signature. It can write a 'cheque' in the format suggested in Figure 1 which can be cashed at an ATM or paid to a shop or transmitted from a home terminal." The "cheque" of Fig. 1 includes a bank identity 1, bank public key 2, expiry data of key 3,

signature of 1-3 by central bank 4, customer identity 5 (cited by the Examiner as a unique identifier), customer public key 6, expiry date of key 7, signature of 5-7 by bank 8, cheque sequence no. 9, transaction type 10, amount of payment 11, currency 12, beneficiary identity 13, description of payment 14, data and time 15, and signature of 9-15 by customer 16 (cited by the Examiner as the unique code generated from the transaction data and the unique identifier).

The Examiner has assumed without support that the signature 16 is generated from transaction data and a unique human identifier. The only teaching with respect to signature 16 by Davies is that it is a "Signature of 9-15 by customer." Davies does not teach how that signature is made. [There is no teaching or suggestion that the information included in the document is used in the creation of the signature] Instead, the signature is affixed to the information included in the document in order to verify the authenticity of that information. The Examiner has simply read this aspect of Applicants' claimed invention into the Davies article.

Further, Davies also fails to teach or suggest formatting the unique code, the transaction data, *and* the unique human identifier to produce a single whole representation of a secure endorsed transaction. As defined, for example, at page 17, line 24, through page 18, line 3, of Applicants' specification, a single whole representation is a combination of the three inputs. This is also depicted, for example, in FIG. 3, where transaction data 210, human identifier 220 and unique code 240 are combined by formatter 310 to produce secure endorsed transaction 320. There is simply no teaching or suggestion in Davies of formatting customer identity 5,

transaction data 9-15, and signature by customer 16 to produce a single whole representation.

Griffith fails to cure the defects in Davies. Griffith fails to teach or suggest the generation of a unique code from transaction data and a unique identifier and the formatting of the unique code, the transaction data and the unique human identifier to produce a single whole representation of a secure endorsed transaction. The Examiner cites individual identifier 100 as the unique human identifier. The transform of the individual identifier 106 is combined by second encoder 104 with the ciphertext verification field 112 to produce media ciphertext 117. This is not a teaching, however, of creating a unique code from transaction data and a unique human identifier. [There is simply no teaching or suggestion of combining individual identifier 100 with transaction data to produce a unique code and then combining the unique code with the transaction data and the unique human identifier to produce a single whole representation of a secure endorsed transaction.]

For at least the reasons expressed above, claim 1 is patentable over Griffith and Davies, alone or in any reasonable combination.

Regarding claims 3, 4 and 25-27, these claims are patentable, at least, in view of their dependence from claim 1.

Regarding claim 5, this claim as amended is directed to a combination of steps including generating unique codes from the transaction data and unique human identifiers and formatting the unique codes, the transaction data, and the unique human identifiers to produce single whole representations of secure endorsed transactions. As discussed above with respect to claim 1, Griffith and Davies, alone or in any reasonable

combination, fail to teach or suggest generating unique codes from the transaction data and unique human identifiers and formatting the unique codes, the transaction data, and the unique human identifiers to produce single whole representations of secure endorsed transactions. Spies fails to cure the defects in the combination of Griffith and Davies. As shown in the transaction process of Fig. 2 of Spies, discussed at column 6, line 60, through column 7, line 28, the encrypted document 36 and encrypted instrument 38 are sent along with the credentials 32(a) produced by credential binding server 26. The endorsement of the transaction, credentials 32(a), is not a unique code generated from the transaction data and a unique human identifier, and is not formatted with transaction data and the unique human identifier to produce a single whole representation of a secure endorsed transaction. For at least these reasons, therefore, claim 5 is patentable over the applied references.

Regarding claims 6, 7, 9, 10, and 20-22 these claims are patentable, at least, in view of their dependence from claim 5.

Regarding claim 11, this claim is directed to a combination of steps including generating a unique code from transaction data, a unique human identifier, and a public key, and generating a digital signature of the unique code using a private key corresponding to the public key. As discussed above with respect to claim 1, Davies teaches a cheque shown in Fig. 1. The Examiner cites customer identity 5 as a unique identifier, elements 9-15 as transaction data, and signature 16 as a unique code. Davies also teaches a bank public key 2 and a customer public key 6. There is simply no teaching in Davies, however, that the signature 16 is generated using data 9-15, customer identity 5 and either bank public key 2 or customer public key 6. The

Examiner has simply read this teaching into the Davies reference. This extension of the Davies reference is not supported, and therefore, is insufficient to maintain the rejection.

Further, claim 11 requires a digital signature of the unique code. As noted above, the Examiner cited signature 16 as the unique code. Claim 11, however, also requires a digital signature of the unique code generated using a private key corresponding to the received public key. It is unclear from the rejection which element of Davies is cited as the digital signature, however, signature 16 is cited by the Examiner as the unique code generated in the previous step, and not as the digital signature of the unique code. Applicants, therefore, respectfully assert that Davies fails to teach or suggest that signature 16 is a digital signature generated using a private key.

Griffith and Spies also fails to teach or suggest generating a unique code from transaction data, a unique human identifier, and a public key, and generating a digital signature of the unique code using a private key corresponding to the public key. Griffith, Spies, and Davies, therefore, alone or in any reasonable combination, therefore, fail to teach or suggest Applicants' claimed invention.

Regarding claim 12, this claim is patentable, at least, in view of its dependence from claim 11. Further, claim 12 requires formatting the digital signature of the unique code, the transaction data, the unique human identifier, and the public key to produce a single whole representation of the secure endorsed transaction. There is no reference in any of the cited documents of performing a step of formatting a digital signature of a unique code, transaction data, a unique human identifier, and a public key to produce a

single whole representation of a secure endorsed transaction. For this additional reason, therefore, claim 12 is patentable over the applied reference.

Regarding claims 13, 14, and 29-31, these claims are patentable, at least, in view of their dependence from claim 11.

Regarding claim 15, this claim is directed to a method of verifying secure endorsed transactions and includes steps of receiving secure endorsed transactions, generating unique codes from the transaction data and unique human identifiers of the secure endorsed transactions, and comparing the unique codes of the received secure endorsed transactions with the generated unique codes.

In presenting the rejection of claim 15, the Examiner relies upon the same arguments presented with respect to the claims directed to generating a secure endorsed transaction. The rejection of claim 15, therefore, is invalid, as none of the elements of a method of verifying secure endorsed transactions is discussed in the rejection of claim 15.

As shown, for example, in FIG. 4 of Applicants' specification, a secure endorsed transaction 320 is received. The transaction data 210 and human identifier 220 is used to generate unique code 410. Unique code 410 is then compared with unique code 240 of the received secure endorsed transaction 320. None of the cited references teaches or suggests comparing a unique code generated from received transaction data and human identifier from the secure endorsed transaction with a unique code received from the secure endorsed transaction.

Regarding the base reference Davies, this reference teaches at page 380

A simple device can be made which connects to the token's interface and can read the document, check the identification number (in the case of human error) and then verify the key. At the same time it should verify the document's signature, for which purpose it reads the signer's public key. The verification of this key can be made to depend on a certificate signed by a bank

This is not a teaching of receiving secure endorsed transactions, generating unique codes from the transaction data and unique human identifiers of the secure endorsed transactions, and comparing the unique codes of the received secure endorsed transactions with the generated unique codes. Any reading of the verification process of Davies to encompass these claimed steps is unreasonable.

Griffith fails to cure the defects in Davies. The process of verifying a transaction is shown, for example, in FIG. 3C of Griffith. The individual identification 313 is checked against files 317 to locate individual security key 318. Individual security key 318 is used by decoder 316 to decode transaction ciphertext 315 and produce other transaction data 319. The only verification is the comparison of individual identifier 313 against the files 317 (see column 4, lines 47-55). There is no generation of a code from transaction data and a unique identifier and then a comparison of the code against a code received with the transaction data and identifier.

Spies also fails to cure the defects in Davies and Griffith. The transaction process of Spies is shown, for example, in Figs. 6 and 7. Step 120 of Spies requires that the verification of the signature is performed using the originator's signing public key, which was received earlier with the originator's credentials. Spies, therefore, also fails to teach or suggest generating a unique codes from transaction data and human

identifiers of secure endorsed transactions and comparing the generated codes against unique codes of the received transactions.

Spies, Davies, and Griffith, therefore, alone or in any reasonable combination, fail to teach or suggest Applicants' claimed invention.

Regarding claim 16, this claim is patentable over the applied references for, at least, essentially the same reasons expressed above with respect to claim 15.

Regarding claims 17 and 18, these claims are patentable, at least, in view of their dependence from claim 16.

Regarding claim 19, this claim is directed to a combination of steps including generating a unique code from a digital signature and a public key of a secure endorsed transaction, generating another unique code from the public key, the human identifier, and the transaction data of the secure endorsed transaction, and comparing the unique codes. As with claim 15 discussed above, all of the elements that are compared in the comparing step are generated from information received in the secure endorsed transaction. Such a process of receiving and comparing is shown in Fig. 7 of Applicants' specification. There is simply no teaching or suggestion in any of the cited references of generating a code using a digital signature and public key received in a secure endorsed transaction, generating a code using transaction data, a human identifier, and a public key received in a secure endorsed transaction, and then comparing the two codes. Claim 19, therefore, is patentable over the applied references.

Regarding claims 23 and 24, as discussed above with respect to claim 1, Davies fails to teach or suggest generating a unique code from transaction data and a unique

identifier. The element of Davies cited by the Examiner as a unique identifier is customer identity 5, the element cited by the Examiner as the unique code is signature 16, and the element cited by the Examiner as transaction data is elements 9-16. Davies, however, does not state that signature 16 is generated from elements 9-16 and customer identity 5. Griffith and Spies fail to cure the defect in Davies. Claim 23, therefore, is patentable over the applied references.

Applicant respectfully requests that this Amendment under 37 C.F.R. § 1.116 be entered by the Examiner, placing claims 1, 3-7, 9-27 and 29-31 in condition for allowance. Applicants submit that the proposed amendments of claims 1, 3-5, 9 and 14 do not raise new issues or necessitate the undertaking of any additional search of the art by the Examiner, since the amendment simply corrects for claim language objected to by the Examiner, corrects the dependency of the claim, or incorporates limitations from a dependent claim. Therefore, this Amendment should allow for immediate action by the Examiner.

Furthermore, Applicants respectfully point out that the final action by the Examiner presented some new arguments as to the application of the art against Applicant's invention. It is respectfully submitted that the entering of the Amendment would allow the Applicants to reply to the final rejections and place the application in condition for allowance.

Finally, Applicants submit that the entry of the amendment would place the application in better form for appeal, should the Examiner dispute the patentability of the pending claims.

In view of the foregoing remarks, Applicants submit that the claimed invention, as amended, is neither anticipated nor rendered obvious in view of the prior art references cited against this application. Applicants therefore request the entry of this Amendment, the Examiner's reconsideration and reexamination of the application, and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

By: Walter J. Hutchiff Reg. No. 24,914
for Jeffrey A. Berkowitz
Reg. No. 36,743

Dated: 11-23-99